

10/18/00
Jc772 U.S. PTO

PATENT
ATTORNEY DOCKET NO.: 83115-002

Jc813 U.S. PTO
09/690818
10/18/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Assistant Commissioner for Patents
BOX PATENT APPLICATION
Washington, D.C. 20231

**TRANSMITTAL FOR A NEWLY EXECUTED ORIGINAL APPLICATION
UNDER 37 C.F.R. §1.53(b)**

This is a request for filing a patent application under 37 C.F.R. §1.53(b) for:

Inventors: Noriaki HASHIMOTO

For: METHOD AND SYSTEM FOR PREVENTING UNAUTHORIZED ACCESS TO A NETWORK

1. This is a new ☒ **Utility** ☐ **Design** ☐ **Plant** patent application.
2. The papers enclosed to obtain a filing date are as follows:
 24 Pages of Application including
 -1- Title Page
 15 Pages of Disclosure
 7 Pages of Claims
 1 Page of Abstract
 6 Sheets of drawings containing 6 Figures
 ☐ The enclosed drawing(s) are photograph(s), and there is also attached a PETITION TO ACCEPT PHOTOGRAPH(S) AS DRAWING(S).
3. Combined Declaration and Power of Attorney
 ☒ Enclosed and is executed by all inventors.
 ☐ Not Enclosed.
 This application is being filed under the provisions of 37 C.F.R. §1.53(f).
 Applicant(s) await notification from the Patent and Trademark Office of the time set for filing the Declaration and paying the filing fees.
4. Language
 ☒ English
 ☐ Non-English
 This application is being filed in accordance with 37 C.F.R. §1.52(d) and §608.01 of the MPEP. Applicant(s) await notification from the Patent and Trademark Office of the time set for filing the verified English translation and the processing fee.

5. Assignment

☐ An assignment of the invention to _____ and a PTO Form-1595, Recordation Form Cover Sheet, are enclosed.

☐ An assignment will be filed at a later date.

6. Priority - foreign applications under 35 U.S.C. §119(a)-(d) or §365(b) or PCT international applications under 35 U.S.C. §365(a) designating at least one country other than the U.S.

☐ Priority of the following foreign application(s) is claimed:

Country	Application No.	Filed

Certified copy: ☐ is attached. ☐ will follow.

7. Priority based on provisional application(s) - 35 U.S.C. §119(e)

☐ Priority of the following provisional application(s) is claimed:

Application No.	Filed

A. Relate Back - 35 U.S.C. §119(e)

☐ Amend the specification by inserting before the first line the sentence:
"This application claims priority of copending provisional application(s)
No. _____ filed on _____."

8. Small entity status

☒ This application is entitled to small status under 37 C.F.R. §§1.9 and 1.27.

9. Fee Calculation (37 C.F.R. § 1.16)

CLAIMS FOR FEE CALCULATION				
	Number Filed	Number Extra	at Rate of	Basic Fee Utility \$710.00 Design \$320.00
Total Claims (37 C.F.R. §1.16(c))	23 - 20 =	3	\$ 18.00 each=	+\$54.00
Independent Claims (37 C.F.R. §1.16(b))	7 - 3 =	4	\$ 80.00 each=	+ \$320.00
Multiple dependent claim(s), if any (37 C.F.R. §1.16(d))			\$ 270.00	+
SUB-TOTAL =				\$ 1,084.00
Reduction by 1/2 for filing by a small entity				-\$ 542.00
TOTAL FILING FEE =				\$ 542.00

10. Fee Payment

☐ Not Enclosed. **NO FEE IS BEING PAID BY CHECK OR DEPOSIT ACCOUNT AT THIS TIME.**

This application is being filed under the provisions of 37 C.F.R. §1.53(f).
Applicant(s) await notification from the Patent and Trademark Office of the time set for filing the Declaration and paying the filing fees.

☒ Enclosed.
A check in the amount of \$542.00 representing the filing fee is enclosed.

11. ☒ **Except** for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account 50-0310. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. §1.136(a)(3).

12. Additional papers enclosed:

- ☐ Change of Correspondence Address
- ☐ Preliminary Amendment
- ☐ Information Disclosure Statement
- ☐ Form PTO- 1449, ___ documents as listed
- ☐ Declaration of Biological Deposit
- ☐ Submission of "Sequence Listing," computer readable copy and/or amendment pertaining thereto for biotechnology invention containing nucleotide and/or amino acid sequence.

Please accord this application an application number and filing date.

Respectfully submitted,

HOGAN & HARTSON, LLP

Dated: October 18, 2000

By: 

Naomi A. Voegthli
Reg. No. 44,371

HOGAN & HARTSON LLP

Columbia Square

555 13th Street, N.W.

Washington, D.C. 20004-1109

Customer No. 24633

UNITED STATES PATENT APPLICATION

OF

NORIAKI HASHIMOTO

FOR

**METHOD AND SYSTEM FOR PREVENTING UNAUTHORIZED ACCESS TO A
NETWORK**

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a method and system for preventing an unauthorized access to a network. The invention uses a plurality of systems and software to protect a network from an unauthorized access.

Discussion of the Related Art

The Internet has experienced, and will continue to experience, an explosive growth. The Internet was originally designed to provide a means for communicating information between public institutions such as universities. However, with the development and provision of user friendly tools for accessing the Internet, the public at large is increasingly turning to the Internet as a source of information and as a means for communicating information. Furthermore, both consumers and companies are turning to the Internet as a means for conducting a variety of financial transactions.

The Internet's success is based partly on the openness of its protocols: TCP (Transmission Control Protocol) and IP (Internet Protocol). Internet protocols operate by breaking up a data stream into data packets. Each data packet includes a data portion and address information. The IP is responsible for transmitting the data packets from the sender to the receiver over a most efficient route. The TCP is responsible for flow management and for ensuring that packet information is correct. Details of the two protocols are available to the public and are known to those skilled in the art.

As the popularity of the Internet grows, so has the number of malicious acts committed

over the Internet. More recently, malicious acts committed over the Internet have caused major disruptions in daily lives of those who rely on the Internet. For example, there have been a number of widely reported malicious acts over the Internet based on computer viruses including the Melissa and Explore.zip viruses and the "I Love You" worm. These viruses spread over computer networks worldwide in a matter of days via the Internet and have caused millions of dollars in damages. Besides computer viruses, the Internet has been used to launch denial of service attacks against popular web sites and vandalize home pages of private and public institutions.

Despite serious economic damages caused by malicious acts over the Internet, efforts by business and government institutions to detect and prevent such acts have not been very effective. This is partly due to the difficulty in tracing identities of those who commit malicious acts over the Internet. In fact, it is widely accepted that one with a moderate amount of technical knowledge and experience relating to the Internet can defeat various measures placed by private and government institutions to detect and prevent malicious acts. For example, it is often difficult to identify individual responsible for committing malicious acts because they can hide their identities relatively easily by altering transmission logs. In fact, they can alter transmission logs to make an innocent party appear responsible for his or her acts.

The ease of altering identities over the Internet facilitates a commission of a malicious act that is difficult, if not impossible, to trace to a responsible party. It is not difficult for one to learn necessary workings of the Internet to commit such untraceable act, since the Internet is based on the premise that protocols and mechanisms used to run it should be available to all. In other words, unlike in the real world, it is much easier for one to learn and control an environment to

escape detection. For example, without leaving one's own desk, one can destroy evidence by manipulating and altering various parts of the Internet. Specifically, one can hide his or her identity by altering transmission logs, altering IP addresses of data packets, or launching malicious acts from a computer that belongs to another. Thus, to prevent untraceable malicious acts and to capture those responsible for such acts, it is important to prevent alteration of identities over the Internet.

Given this relative ease of committing untraceable malicious acts and the difficulty in capturing those responsible for them, it becomes increasingly important to prevent malicious acts over the Internet from becoming untraceable. The best way to do so is to prevent those who commit untraceable malicious acts from connecting to the Internet. In particular, it is important to prevent an access to the Internet by those who try to mask their identities by altering an originating IP address of a data packet that they send. Thus, there is a need for providing a system and method for preventing an unauthorized access to the Internet or a network by blocking a data packet with an inaccurate or altered IP address information in order to increase overall network security.

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a method and system for preventing an unauthorized access to a network. Specifically, the present invention is directed to a method and system for preventing an access to a network when an originating IP address of a data packet received from a computer does not match the IP address assigned to that computer.

To achieve these and other advantages and in accordance with the purpose of the present invention, as embodied and broadly described, an access control system for preventing an unauthorized access to a computer via a user computer connected to the network includes a memory and a microprocessor. The memory contains an IP address assigned to the user computer. The microprocessor is programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

In another aspect, the invention includes an access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system. The access control system has a memory and a microprocessor and is located between the user computer and the host computer system. The memory contains an IP address assigned to the user computer. The microprocessor is programmed to terminate a connection between the user computer and the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer contained in the memory.

In another aspect, the invention includes a method for preventing an unauthorized access to a network via a user computer that is connected to the network and to an access control system. The method includes storing an IP address of the user computer in a memory of the access control system and receiving a data packet from the user computer. It further includes comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system and denying the user computer an access to the

network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

In yet another aspect, the invention includes a method for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system that is connected to an access control system. The method includes storing an IP address of the user computer in a memory of the access control system and receiving a data packet from the user computer. It further includes comparing an originating IP address of the data packet with the IP address of the user computer in the memory of the access control system and terminating a connection between the user computer and the host computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

In a further aspect, the invention includes a secure network including a host computer system connected to the secure network, an access control system connecting to the host computer system, and a user computer connected to the host computer system. The user computer is capable of accessing the secure network through the host computer system. The access control system has a memory that contains an IP address of the user computer. It is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in its memory.

In another aspect, the invention includes a secure network that includes a user computer connected to the secure network and an access control system. The access control system has a

memory that contains an IP address of the user computer. It is programmed to deny the user computer an access to the secure network when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in its memory.

5 Finally, the invention also includes an access control system for preventing an unauthorized access to a network via a user computer connected to the network. The access control system includes a memory and a comparator structure. The memory contains an IP address of the user computer. The comparator structure is capable of terminating a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
9460
9465
9470
9475
9480
9485
9490
9495
9500
9505
9510
9515
9520
9525
9530
9535
9540
9545
9550
9555
9560
9565
9570
9575
9580
9585
9590
9595
9600
9605
9610
9615
9620
9625
9630
9635
9640
9645
9650
9655
9660
9665
9670
9675
9680
9685
9690
9695
9700
9705
9710
9715
9720
9725
9730
9735
9740
9745
9750
9755
9760
9765
9770
9775
9780
9785
9790
9795
9800
9805
9810
9815
9820
9825
9830
9835
9840
9845
9850
9855
9860
9865
9870
9875
9880
9885
9890
9895
9900
9905
9910
9915
9920
9925
9930
9935
9940
9945
9950
9955
9960
9965
9970
9975
9980
9985
9990
9995
10000
10005
10010
10015
10020
10025
10030
10035
10040
10045
10050
10055
10060
10065
10070
10075
10080
10085
10090
10095
10100
10105
10110
10115
10120
10125
10130
10135
10140
10145
10150
10155
10160
10165
10170
10175
10180
10185
10190
10195
10200
10205
10210
10215
10220
10225
10230
10235
10240
10245
10250
10

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention, and together with the description serve to explain the principles of the invention. In the drawings:

FIG. 1 is a diagram of one embodiment of a secure network using access control systems of the present invention;

FIG. 2 is a diagram of a second embodiment of a secure network using access control systems of the present invention;

FIG. 3 is a diagram of a third embodiment of a secure network using access control systems of the present invention;

FIG. 4 is a diagram of an embodiment of an access control system of the present invention;

FIG. 5 is a flow chart depicting an embodiment of one aspect of an operation performed by an access control system of the present invention; and

FIG. 6 is a diagram of an alternative embodiment of an access control system of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

With reference to FIG. 1, one embodiment of a secure network using access control systems of the present invention includes a user computer 100 connected to a host computer system 102 via Public Switched Telephone Network (PSTN) 101. The user computer 100 accesses the Internet 103 via the host computer system 102. An Internet service provider typically operates the host computer system 102. The host computer system 102 comprises a plurality of modems (102B, 102C, and 102D), a plurality of access control systems (102E, 102F, and 102G), and an access server 102A.

An access control system is typically located within or close to the host computer system 102, so that a user has no physical access to it. Moreover, it is preferable that a user has no remote access to an access control system. FIG. 1 shows the plurality of access control systems (102E, 102F, and 102G) installed between the plurality of modems (102B, 102C, and 102D) and the access server 102A. While FIG. 1 shows one access control system per one modem, one access control system may be connected to more than one modem. Alternatively, one modem may be connected to more than one access control system. Further, the access control systems (102E, 102F, and 102G) may be installed within each of the modems (102B, 102C, and 102D) of the host computer system 102 either as hardware or software. One or more access control systems may also be installed within the access server 102A either as hardware or software.

The host computer system 102 typically assigns one of the modems connected to the access server 102A to the user computer 100. For example, the user computer 100 might access the Internet 103 using the modem 102B. Then, the access control system 102E would contain the IP address assigned to the user computer 100 and would monitor data packets sent from the user

computer 100. When the stored IP address does not match an originating IP address of a data packet received from the user computer 100 via the modem 102B, the access control system 102E would terminate the connection between the user computer 100 and the host computer system 102. In other words, the user computer 100 would no longer be able to access the Internet 103. To resume sending data packets to the Internet 103, the user computer would have to reestablish a connection, for example, by logging onto the host computer system 102.

The access control systems 102E, 102F, and 102G may terminate the connection between the user computer 100 and the host computer system 102 by electrically cutting off the connection between them or by filtering out data packets sent from the user computer 100. Alternatively, they may issue commands to an appropriate modem or the access server 102A, so that either the modem or the access server 102A would terminate the connection between the user computer 100 and the host computer system 102. Other methods of terminating the connection between the user computer 100 and the host computer system 102 would be known to those skilled in the art and are within the scope of this invention.

FIG. 4 depicts one embodiment of an access control system 400 that is implemented with separate hardware. As started previously, an access control system may also be implemented by software. When implemented by software, it may run on a separate hardware, a user computer, a host computer system, or other peripherals used to access the Internet such as a modem or a hub. Further, while FIG. 4 depicts a memory 400A and a microprocessor 400B as two separate components, this separation is not required. For example, one may use an internal memory of the microprocessor 400B instead of a separate memory.

In FIG. 4, the access control system 400 is connected to a user computer 401 and a host computer system 402 via network cables 403 and 404. The access control system 400 has the memory 400A and the microprocessor 400B. The memory 400A contains an IP address assigned to the user computer 401, if any. The microprocessor 400B is programmed so that it compares an originating IP address of a data packet received from the user computer 401 with the IP address of the user computer stored in the memory 400A. The access control system 400 discards the data packet, if the two IP addresses are not the same, or if its memory does not contain any address information of the user computer 401. It also causes the connection between the user computer 401 and the host computer system 402 to terminate. Upon the termination of the connection between the user computer 401 and the host computer system 402, the IP address of the user computer 401 may be deleted from the memory 400A. If an IP address to the user computer 401 is dynamically assigned, the memory 400A is updated when a new IP address is assigned to the user computer 401. If the user computer 401 has a permanent IP address, the memory 400A contains that address.

While the FIG. 4 shows the access control system 400 with two network connections 403 and 404, it may have more than two connections. In any case, it is preferable that the access control system supports various types of networks such as Ethernet (IEEE 802.3) and a serial network (RS-232C). Furthermore, the access control system may be programmed so that it is equipped with additional filtering capabilities to allow filtering of data packets based on a factor other than an originating IP address. It would be desirable to program the access control system so that its filtering parameters may be altered in real time and/or remotely.

Typically, an IP address is assigned to the user computer 401 by the host computer system 402 when the connection between the user computer 401 and the host computer system 402 is established. Protocols used to establish the connection between the two computers include Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), and any other protocols that are used for dial-up connections. Additional protocols include Dynamic Host Configuration Protocol (DHCP), which may be used when the host computer system 402 functions as a DHCP server in a local area network.

FIG. 6 shows another embodiment of an access control system of the present invention. Under this implementation, the access control system comprises a memory 600 and a comparator structure with a comparator 602 and an AND gate 602. The memory 600 contains IP addresses of one or more user computers connected to the access control system. When the access control system receives a data packet from a user computer, the comparator 601 compares an originating IP address of the data packet with an IP address of the user computer contained in the memory 600. If the two addresses are the same, the AND gate 602 forwards the data packet. If they are different, it blocks the data packet. In addition to blocking the data packet, it may also cause the connection between the user computer and a host computer system to terminate.

FIG. 5 is used to explain one aspect of the operation of a preferred embodiment of an access control system. At step 500, an IP address assigned to a user computer is stored in the memory of the access control system. If the IP address of the user computer changes periodically this step needs to be repeated whenever a new IP address is assigned to the user computer. The step 500 typically occurs when a connection between the user computer and a host computer

system is established and the host computer system assigns an IP address to the user computer. If a permanent IP address is assigned to the user computer, this step may need to be executed only once.

At steps 501 and 502, an originating IP address of a data packet received from the user computer is compared with the IP address of the user computer stored in the memory. If the two IP addresses are the same, the data packet is sent to a network, which typically is the Internet, at step 503. More specifically, the access control system may forward the data packet to an access server of a host computer system for forwarding to the Internet. If the two IP addresses do not match, the access control system causes a connection between the user computer and the host computer system to terminate at step 504. The access control system itself may cause the termination of the connection by electrically cutting of the connection between the user computer and the host computer system or by filtering out data packets from the user computer.

Alternatively, it may issue commands so that the host computer system would terminate the connection with the user computer. Other methods of terminating the connection between the user computer and the host computer system would be known to those skilled in the art and thus are within the scope of the present invention.

Upon the termination of the connection, the access control system may delete the IP address of the user computer from the memory at 505. The IP address of the user computer may also be deleted when the user computer terminates the connection with the host computer system.

FIG. 2 depicts another embodiment of a secure network using access control systems of the present invention. A host computer system 202 includes a hub 202A and access control

systems 202B and 202C. User computers 200 and 201 are connected to the hub 202A, for example, via a local area network. The hub 202A provides an access to the Internet 203. In other words, the user computers 200 and 201 access the Internet 203 via the hub 202A.

In FIG. 2, the access control systems 202B and 202C are located between the hub 202A and the user computers 200 and 201, respectively. They may also be implemented within the hub 202A or another system, such as a system provided by an Internet service provider, to which the hub 202A is connected, either as hardware or software. In either case, the access control systems should be implemented so that they would not be physically accessible to users without a proper authorization.

The access control systems 202B and 202C are responsible for data packets sent from the computers 200 and 201, respectively. For example, the access control system 202B would contain an IP address assigned to the user computer 200 and would terminate the connection between the user computer 200 and the hub 202A, when an originating IP address of a data packet from the user computer 200 does not match the stored IP address.

While the diagram depicts the network configured in a star topology with one hub (202A), other network configurations would be known to those skilled in the art and are within the scope of this invention.

FIG. 3 depicts yet another implementation of a secure network using access control systems of the present invention. User computers 300, 301, and 302 access the Internet 307 though an access server 306. An Internet service provider may operate the access server 306. Alternatively, the access server 306 may be connected to a system operated by an Internet service

provider. While this implementation depicts the user computers (300, 301, and 302) connected via a bus network, other network configurations such as a ring network may be used to implement the secure network of the present invention.

In FIG. 3, access control systems 303, 304 and 305 reside outside the user computers 300, 301, and 302. They are located between each user computer and the access server 306. The access control systems 303, 304, and 305 may also be located within the user computers 300, 301, and 302. Alternatively, one or more access control system may be located within the access server 306.

Unlike the implementations in FIGS. 1 and 2, the access control systems 303, 304, and 305 in FIG. 3 are located near the user computers 300, 301, and 302. In other words, users have a physical access to them. Thus, it may be necessary to add capabilities to detect a physical tampering of the access control systems and to disable an access to the Internet upon a detection of any physical tampering.

Just like an access control system attached to a host computer system, the access control systems (303, 304, and 305) in FIG. 3 are programmed to terminate connections between the user computers (300, 301, and 302) and the access server 306, when they receive a data packet whose originating IP address does not match the stored IP address. Each access control system is responsible for monitoring an originating IP address of each data packet sent from a user computer connected to it. For example, the access control system 303 checks an originating IP address of each data packet sent from the user computer 300. Upon detecting a mismatch between an originating IP address and the stored IP address, the access control system 303, for

example, terminates the connection between the user computer 300 and the access server 306 to prevent a transmission of any subsequent data packet from the user computer to the Internet.

This may be achieved, for example, by electrically cutting of the connection between the user computer 300 and the access server 306 or by filtering out data packets received from the user

5 computer 300. Alternatively, the access control system 303 may issue appropriate commands to the user computer 300 or the access server 306 to terminate the connection.

It will be apparent to those skilled in the art that various modifications and variations can be made in the method and system for preventing unauthorized access to a network of the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What Is Claimed Is:

1. An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising;

a memory containing an IP address assigned to the user computer; and

5 a microprocessor programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

10 2. The access control system of claim 1, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

15 3. The access control system of claim 1, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

4. The access control system of claim 1, wherein the memory is a part of the microprocessor.

5. An access control system for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system, the system comprising;
a memory containing an IP address assigned to the user computer; and
a microprocessor programmed to terminate a connection between the user computer and
5 the host computer system when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory,

wherein the access control system is located between the user computer and the host computer system.

10 6. The access control system of claim 5, wherein the microprocessor is further programmed to delete the IP address of the user computer from the memory when the originating IP address of the data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

15 7. The access control system of claim 5, wherein the microprocessor is further programmed to update the IP address of the user computer contained in the memory.

20 8. The access control system of claim 5, wherein the memory is a part of the microprocessor.

9. A method for preventing an unauthorized access to a network via a user computer which is connected to the network and to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

receiving a data packet from the user computer;

5 comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

10 10. The method of claim 9, wherein the denying step includes terminating the connection between the user computer and the network.

11. The method of claim 9, further comprising updating the IP address of the user computer stored in the memory of the access control system.

15 12. The method of claim 9, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

13. A method for preventing an unauthorized access to a network via a user computer connected to the network through a host computer system which is connected to an access control system, the method comprising:

storing an IP address of the user computer in a memory of the access control system;

5 receiving a data packet from the user computer;

comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory of the access control system; and

terminating a connection between the user computer and the host computer system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

14. The method of claim 13, further comprising deleting the IP address of the user computer from the memory of the access control system if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory of the access control system.

15. The method of claim 13, further comprising updating the IP address of the user computer stored in the memory of the access control system.

16. A secure network comprising:

a host computer system connected to the secure network;

an access control system connected to the host computer system and having a memory;

and

a user computer connected to the host computer system capable of accessing the secure network through the host computer system,

wherein the memory of the access control system contains an IP address assigned to the user computer, and wherein the access control system is programmed to terminate a connection between the host computer system and the user computer when an originating IP address of a data packet sent from the user computer for transmission to a node in the secure network does not match the IP address of the user computer contained in the memory of the access control system.

17. The secure network of claim 16, wherein the user computer and the host computer system are connected via a Public Switched Telephone Network.

18. The secure network of claim 16, wherein the host computer system comprises an access server and a plurality of modems and wherein the access control system is located between the access server and the plurality of modems.

19. The secure network of claim 16, wherein the host computer system and the user computer are connected via a local area network.

20. A secure network comprising:

a user computer connected to the secure network; and

an access control system connected to the user computer and having a memory,

wherein the memory of the access control system contains an IP address assigned to the

user computer, and wherein the access control system is programmed to deny the user computer

an access to the secure network when an originating IP address of a data packet sent from the

user computer for transmission to a node in the secure network does not match the IP address of

the user computer contained in the memory of the access control system.

21. An access control system for preventing an unauthorized access to a network via a user computer connected to the network, the system comprising;

a memory containing an IP address assigned to the user computer; and

a comparator structure capable of terminating a connection between the user computer

and the network when an originating IP address of a data packet received from the user computer does not match the IP address assigned to the user computer that is contained in the memory.

22. The access control system of claim 21, wherein a comparator structure comprises a microprocessor.

23. The access control system of claim 22, wherein the memory is a part of the microprocessor.

ABSTRACT OF THE DISCLOSURE

A method and system for preventing an unauthorized access to a network via a user computer. The system includes a memory containing an IP address of the user computer and a microprocessor. The microprocessor is programmed to terminate a connection between the user computer and the network when an originating IP address of a data packet received from the user computer does not match the IP address of the user computer contained in the memory. The method uses a user computer connected to a network and an access control system. It includes storing an IP address of the user computer in a memory of the access control system, receiving a data packet from the user computer, and comparing an originating IP address of the data packet with the IP address of the user computer stored in the memory. The method further includes denying the user computer an access to the network if the originating IP address of the data packet is different from the IP address of the user computer stored in the memory.

005"01" 8180960

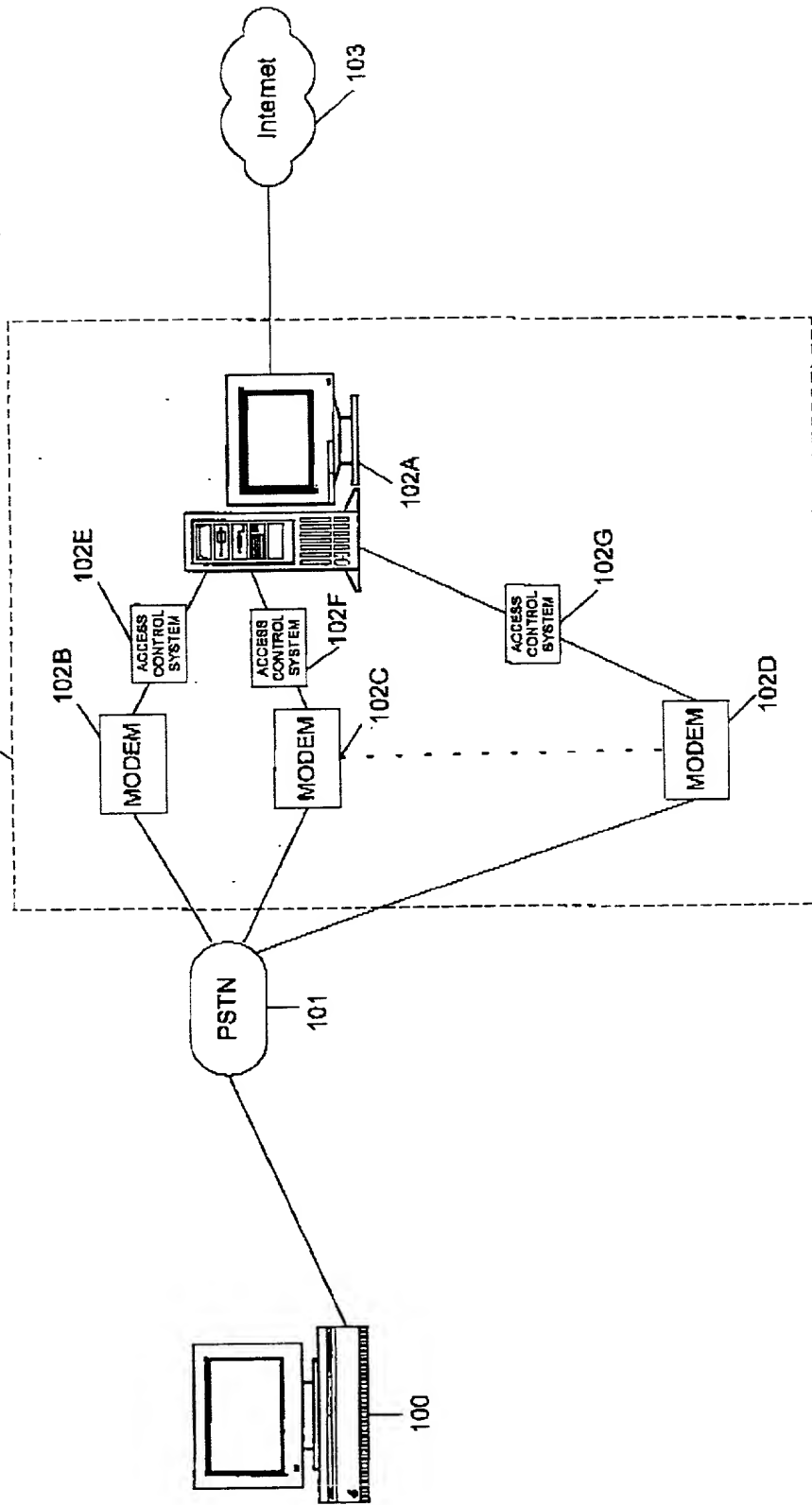


FIG. 1

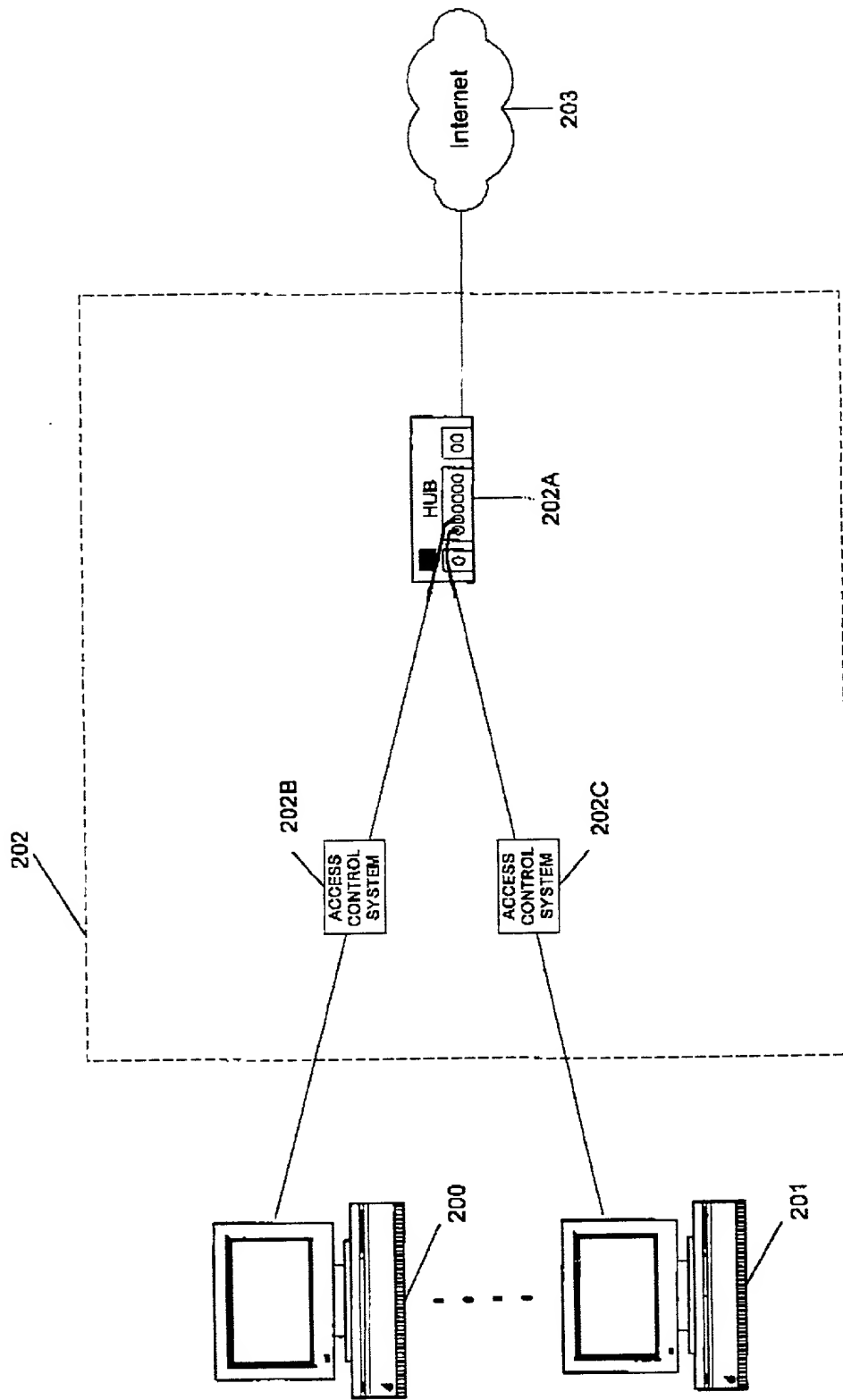


FIG. 2

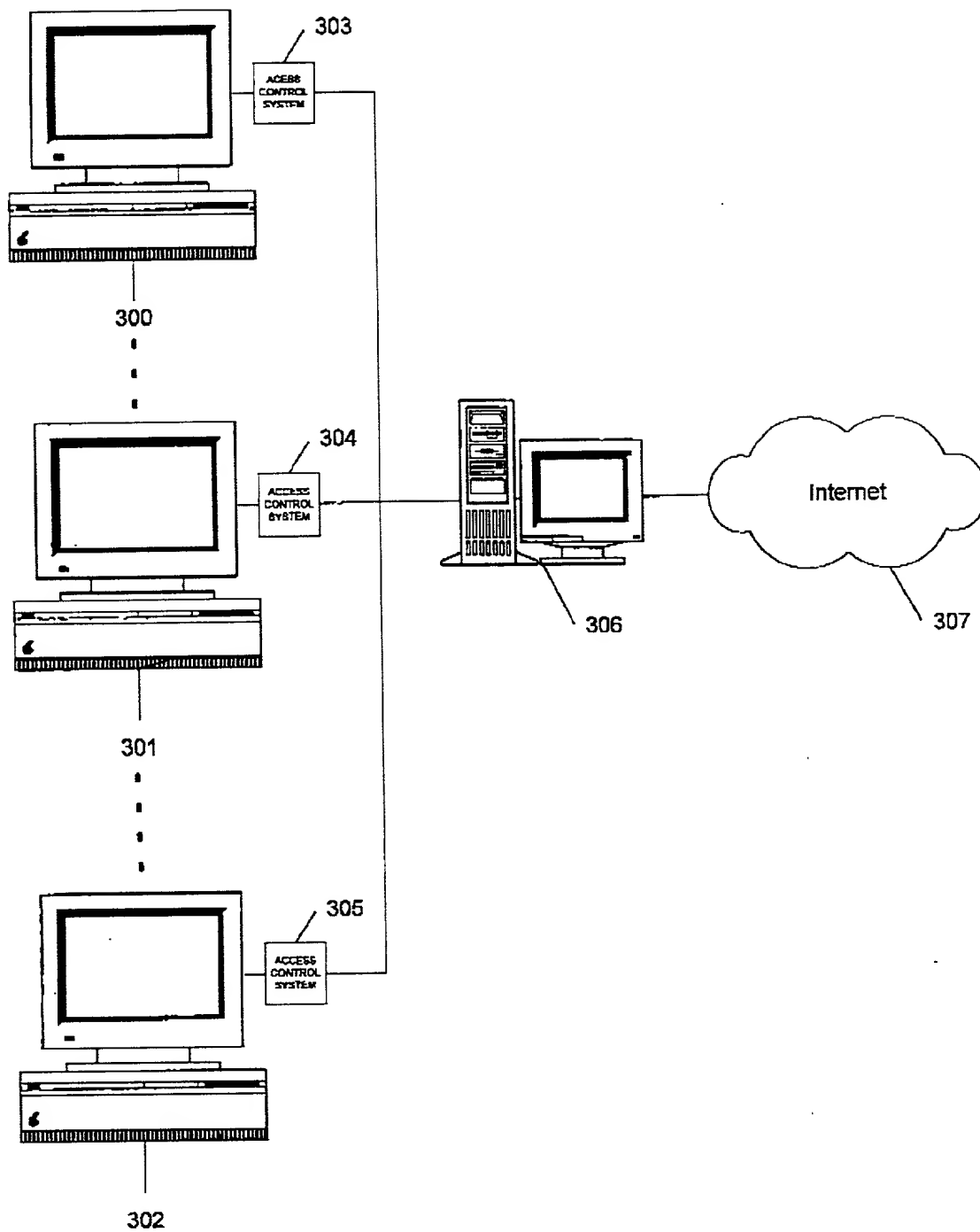


FIG. 3

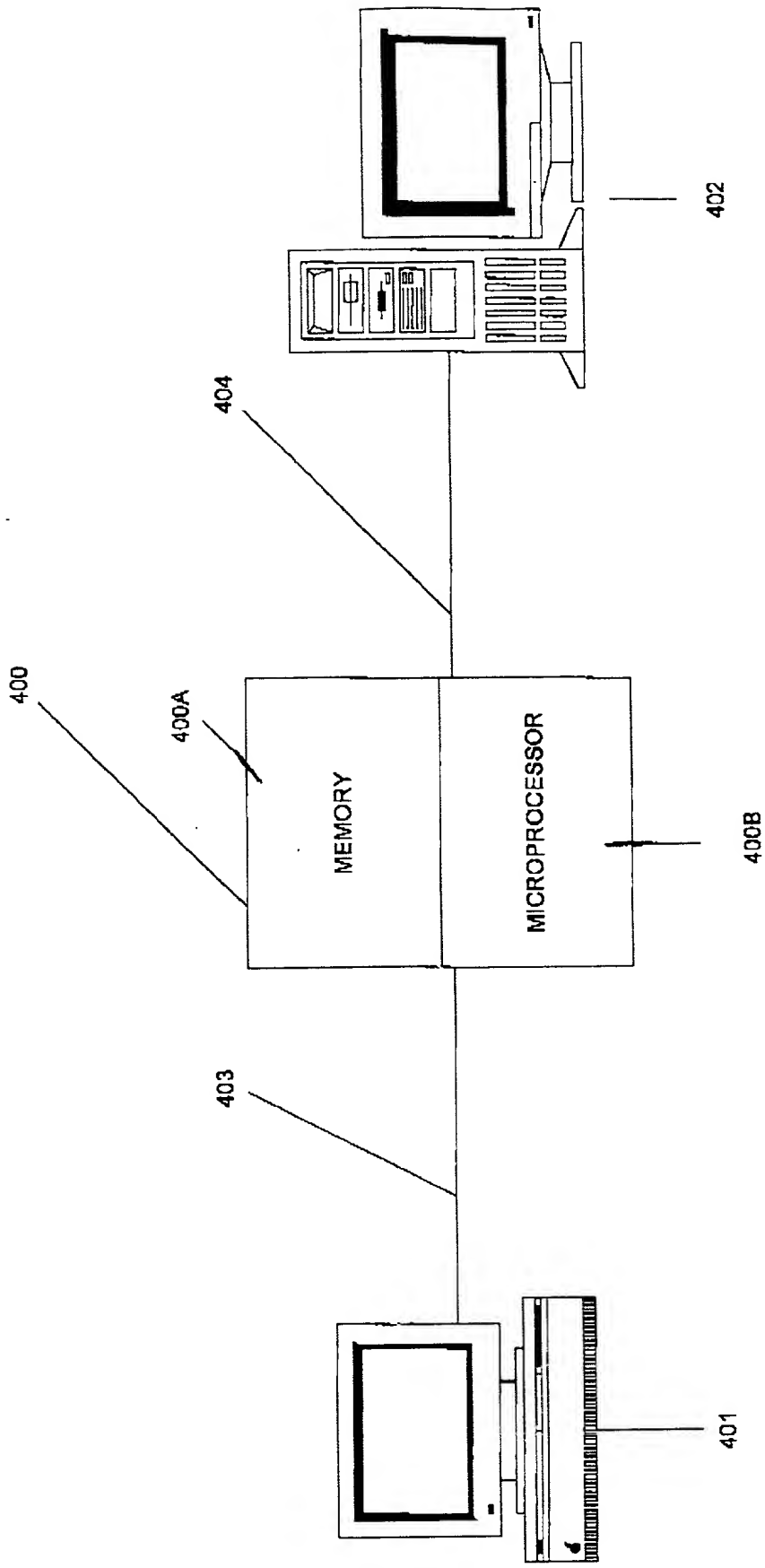


FIG. 4

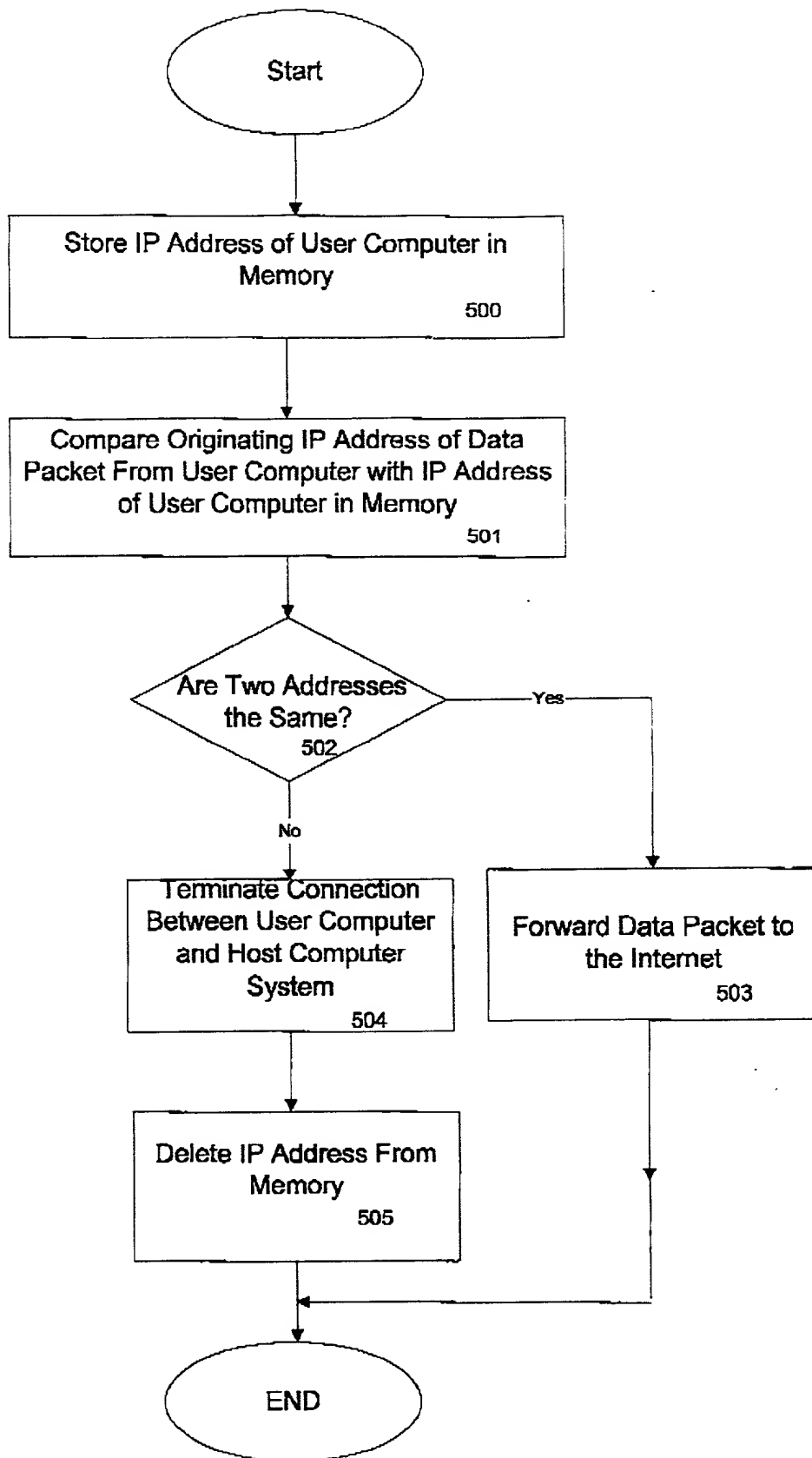


FIG. 5

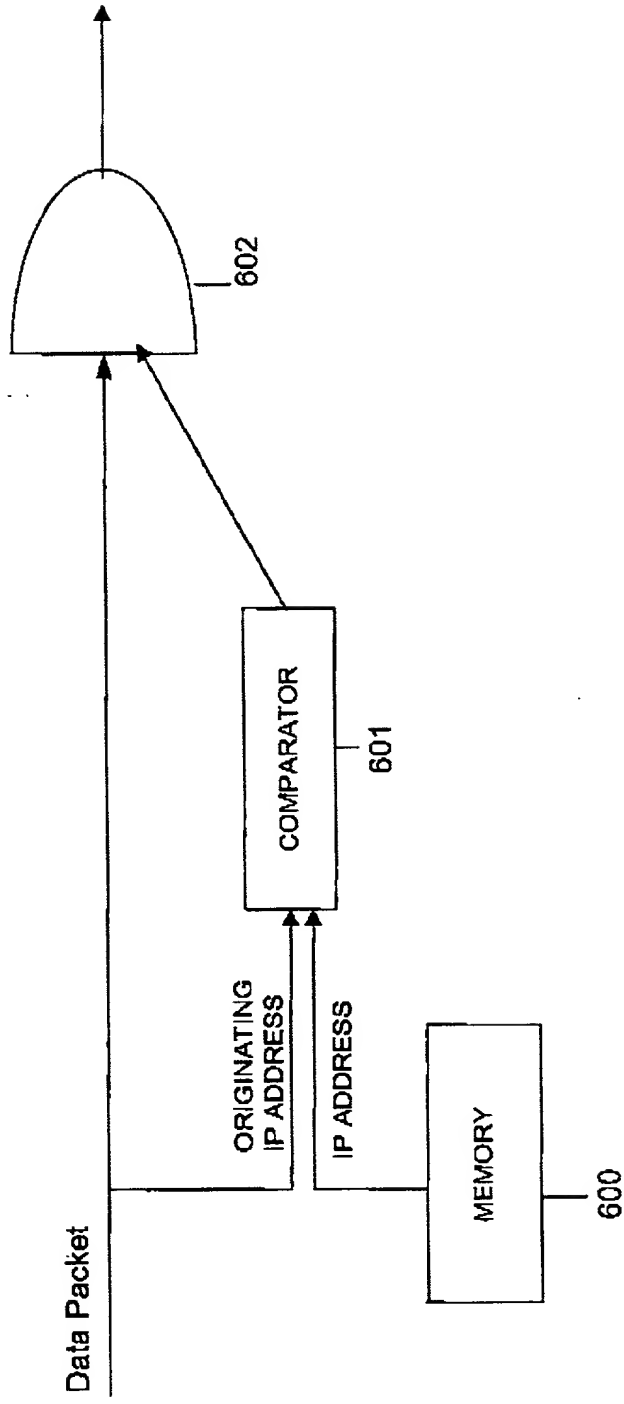


FIG. 6

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

ATTORNEY DOCKET NO.: 83115-002

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND SYSTEM FOR PREVENTING UNAUTHORIZED ACCESS TO A NETWORK

the specification of which:

☒ is attached hereto; or☐ was filed as United States application Serial No. _____ on _____ and was amended on _____ (if applicable); or

was filed as PCT international application Number _____ on _____ and was amended under PCT Article 19 on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office information which is material to the patentability of claims presented in this application in accordance with Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate or § 365(a) of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN APPLICATION(S):

COUNTRY (if PCT, indicate PCT)	APPLICATION NUMBER	DATE OF FILING (day, month, year)	PRIORITY CLAIMED
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the benefits under Title 35, United States Code §119(e) of any United States provisional application(s) listed below:

U.S. PROVISIONAL APPLICATIONS

U.S. PROVISIONAL APPLICATION NO.	U.S. FILING DATE

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or § 365(c) of any PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to the patentability of claims presented in this application in accordance with Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S. FOR BENEFIT:

U.S. APPLICATIONS		STATUS (Check One)		
U.S. APPLICATION NO.	U.S. FILING DATE	PATENTED	PENDING	ABANDONED

POWER OF ATTORNEY: As a named inventor, I hereby appoint the registered practitioners of Hogan & Hartson LLP included in the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to that Customer Number.

Customer Number: 24633

Direct Telephone Calls To:
(name and telephone number)

NAOMI ABE VOEGTLI
202-637-5891

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF SOLE INVENTOR	Noriaki HASHIMOTO		
RESIDENCE & CITIZENSHIP	Kawaguchi-shi, Saitama-ken, JAPAN	COUNTRY OF CITIZENSHIP JAPAN	
POST OFFICE ADDRESS	2231-3 Angyoryo, Negishi, Kawaguchi-shi, Saitama-ken 333-0834 JAPAN		
SOLE INVENTOR'S SIGNATURE	<i>Noriaki Hashimoto</i>		DATE 17th/Oct/2000